(2 ½ Hours) **[Total Marks: 75]**

N.B. 1) All questions are compulsory.
2) Figures to the right indicate marks.
3) Illustrations, in-depth answers and diagrams will be appreciated.
4) Mixing of sub-questions is not allowed.

Q. 1 Attempt All(Each of 5Marks) **(15M)**

(a) Multiple Choice Question

i) Message ________ means that the data must arrive at the receiver exactly as it is sent. a) Access Control b) Non repudiation c) Masquerade d) Integrity

ii) Which one of the following is passive attack?
a) Masquerade b) Traffic analysis c) Repudiation d) Replay

iii) A firewall is specific form of a) router b) bridge c) Operating System d) Architecture

iv) To sign a document digitally we need a) Sender's Private key b) Sender's Public key c) Receiver's Private key d) Receiver's Public key

v) DES is an acronym for. a) Data encryption Standard b) Digital encryption Standard c) Data encryption System d) Double encryption Standard

(b) Fill in the blanks

(Message Digest, crossover ,encrypted, Transport ,asymmetric cryptography, mutation)

i) For confidentiality, data to be sent is____________.

ii) A polymorphic virus undergoes __________.

iii) SHA -512 is a ____________ algorithm.

iv) Digital signature uses __________ cryptography.

v) SSL is a _______ Layer protocol. Transport

(c) Short Answers

i) Define block cipher?

ii) What is Fiestel cipher?

iii) List out any two virus countermeasures.

iv) List out the functions used for rounds of AES?

v) Define Honeypot.

Q. 2 Attempt the following (Any THREE)(Each of 5Marks) **(15M)**

(a) List and explain different categories of security services.

(b) Explain Vigenere cipher giving proper example.

(c) Write an overview of DES algorithm.

(d) Explain ECB model of operation of block cipher.

(e) Explain Asymmetric cryptography with its application.

(f) Define security attack. Explain its different types?

Q. 3 Attempt the following (Any THREE) (Each of 5Marks) (15M)

(a) Differentiate between stream cipher and block cipher.

(b) Discuss MAC in detail.

(c) Explain digital signature process.

(d) Discuss Diffie Hellman key exchange process.

(e) Write a short note on Kerberos.

(f) Explain the concept of Digital Certificate in detail.

Q. 4 Attempt the following (Any THREE) (Each of 5Marks) (15)

(a) Explain PGP with different services offered by it.

(b) Discuss SSL handshaking protocol in detail.

(c) Define Intrusion. Explain different approaches of Intrusion detection.

(d) Define malicious software. Explain different types of viruses.

(e) Explain capabilities and limitations of firewall.

(f) Explain Secure Electronic Transaction.

Q. 5 Attempt the following (Any THREE) (Each of 5Marks) (15)

(a) Explain different aspects of Network security.

(b) Explain different modes of operations of IPSec protocol.

(c) Explain Man in middle attack.

(d) Explain lifecycle of virus.

(e) Encrypt NOTHING IS AS IT SEEMS and decrypt MKHSE LWYAE ATSOL using Rail Fence cipher.
